Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Артеменков Михаил Николаевич
Должность: Ректор
Дата подписания: 21.10.2026 15:51:46
Уникальный программный ключ:
a63b74166e8f4fc17bd1e0462725f79e393bfdf9

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Смоленский государственный университет»

«Утверждаю»
Проректор по учебно-
методической деятельности
Ю.А. Устименко
«25» декабря 2025 г.

Рабочая программа дисциплины
ОП.11 Информационная безопасность

Специальность: 09.02.13 Интеграция решений с применением технологий искусственного интеллекта
Квалификация выпускника: специалист по работе с искусственным интеллектом
Нормативный срок обучения: 3 года 10 месяцев
Форма обучения: очная

Смоленск
2025

Содержание:

1. Паспорт рабочей программы дисциплины
1.1. Область применения программы
1.2 Место дисциплины в структуре ППССЗ
1.3 Общая характеристика учебной дисциплины
2. Структура и содержание дисциплины
2.1 Объем и виды учебной работы
2.2 Тематический план и содержание дисциплины
3. Условия реализации дисциплины
3.1 Требования к материально-техническому обеспечению
3.2. Информационное обеспечение реализации дисциплины
3.3 Программное обеспечение реализации дисциплины
4. Контроль и оценка результатов освоения дисциплины

1. Паспорт рабочей программы предмета

Целью реализации программы является достижение выпускниками планируемых результатов: компетенций и компетентностей, определяемых личностными, семейными, общественными, государственными потребностями и возможностями обучающегося старшего школьного возраста, индивидуальной образовательной траекторией его развития и состоянием здоровья.

1.1 Область применения программы

Реализация среднего профессионального образования по программе подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта, утвержденного приказом Минпросвещения России от 24.12.2024 г. N 1025.

1.2. Место дисциплины в структуре образовательной программы

Дисциплина ОП.11 Информационная безопасность входит в часть, формируемую участниками образовательных отношений (вариативная часть), общепрофессионального цикла учебного плана образовательной программы в соответствии с ФГОС СПО по специальности 09.02.13 Интеграция решений с применением технологий искусственного интеллекта. Особое значение дисциплина имеет при формировании и развитии следующих компетенций в соответствии с ФГОС СПО: ОК 01.; ОК 02.; ОК 03.; ОК 09.; ПК 2.3.

1.3 Общая характеристика дисциплины

Цель дисциплины: формирование знаний об основах информационной безопасности, освоение принципов защиты информации на всех этапах её жизненного цикла, развитие навыков применения нормативных требований, методов и средств обеспечения безопасности при работе с данными и информационными системами, включая системы с использованием искусственного интеллекта.

Задачи дисциплины:

– Сформировать системное представление об угрозах информационной безопасности, актуальных для современных информационных систем и технологий ИИ (атаки на данные, модели, интеллектуальную собственность).

– Освоить основные понятия, принципы (конфиденциальность, целостность, доступность) и отечественную нормативно-правовую базу в области защиты информации.

– Развить умение анализировать риски информационной безопасности на типовых объектах защиты (персональные данные, коммерческая тайна, базы данных, алгоритмы).

– Научить применять базовые организационные и технические меры защиты информации на уровне пользователя и администратора (управление доступом, антивирусная защита, резервное копирование, основы криптографии).

– Сформировать навыки проведения элементарного аудита защищенности информационных систем, в частности систем управления базами данных, на соответствие установленным регламентам.

Планируемые результаты освоения дисциплины

В результате освоения учебной дисциплины обучающийся должен **знать**:

– З1 – основные понятия, цели и принципы информационной безопасности (конфиденциальность, целостность, доступность, аутентичность, неотказуемость);

– З2 – классификацию угроз и уязвимостей информационных систем, источники и виды угроз (внутренние/внешние, преднамеренные/непреднамеренные), типы атак (социальная инженерия, вредоносное ПО, DDoS);

– З3 – основы российского законодательства в области ИБ;

– З4 – модели и политики управления доступом (DAC, MAC, RBAC), принципы аутентификации, авторизации и аудита (AAA);

– З5 – базовые методы и средства криптографической защиты информации (шифрование, ЭЦП, хеширование), их применение для обеспечения конфиденциальности и целостности;

– З6 – принципы обеспечения безопасности на различных уровнях: физический, аппаратный, уровень ОС, сетевой, прикладной;

– З7 – методику проведения базового аудита безопасности, структуру и содержание типовых регламентов по защите информации, стандартов.

В результате освоения дисциплины обучающийся должен **уметь:**

– У1 – идентифицировать основные активы (данные, системы, сервисы) и анализировать связанные с ними риски информационной безопасности в контексте профессиональной деятельности;

– У2 – применять базовые меры защиты на уровне рабочей станции и пользователя: настройка парольной политики, работа с антивирусным ПО, настройка брандмауэра, безопасное использование съемных носителей;

– У3 – работать с нормативной документацией (политики ИБ, регламенты, инструкции) на русском языке, понимать ключевые положения стандартов ИБ на английском языке;

– У4 – использовать основные криптографические средства (средства шифрования дисков, создания ЭЦП, проверки хеш-сумм) для защиты данных;

– У5 – проводить элементарную проверку (аудит) настроек безопасности СУБД на предмет соответствия базовым требованиям (сложность паролей, права доступа, журналирование);

– У6 – разрабатывать и оформлять простейшие организационно-распорядительные документы в области ИБ (инструкция пользователя, регламент обращения с конфиденциальной информацией).

В результате освоения дисциплины обучающийся должен иметь **практический опыт:**

– П1 – оценки защищенности информационной системы или её компонента по заданным критериям;

– П2 – применения полученных знаний для обеспечения безопасной работы с персональными и конфиденциальными данными в учебных и модельных профессиональных ситуациях;

– П3 – использования нормативно-правовой базы и профессиональной документации для обоснования принимаемых решений в области ИБ;

– П4 – проведения элементарных аудиторских проверок настроек систем (в частности, СУБД) с использованием чек-листов и регламентов.

Результатом освоения дисциплины является овладение обучающимися общими (ОК) и профессиональными (ПК) компетенциями:

Код	Наименование результата обучения
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках
ПК 2.3	Проводить аудит систем безопасности баз данных с использованием регламентов по защите информации

2. Структура и содержание предмета

2.1 Объем и виды учебной работы

Вид учебной работы	Объем, академические часы
3 семестр	
Максимальная учебная нагрузка (всего)	64
Обязательная аудиторная учебная нагрузка (всего)	48
Лекции	16
Лабораторные занятия/ практическая подготовка	32/32
Самостоятельная работа обучающегося	4
Форма промежуточной аттестации: экзамен	12
Всего часов по предмету	64

2.2 Тематический план и содержание предмета

Наименование разделов и тем	**Содержание учебного материала и формы организации деятельности обучающихся**	**Объем, акад. ч. / в том числе в форме практической подготовки, ак.ч.**	**Коды компетенций, формированию которых способствует элемент программы**
3 семестр			
Раздел 1. Основы и нормативное регулирование информационной безопасности			
Тема 1.1. Основные понятия, принципы и угрозы ИБ	Концепция информационной безопасности: конфиденциальность, целостность, доступность (CIA Triad). Классификация угроз и атак: внутренние/внешние,	**6** **из них:**	З1, З2, У1, П1, ОК 01

	пассивные/активные, социальная инженерия, вредоносное ПО. Понятие уязвимости, риска и актива. Модели нарушителя.		
	Лекционные занятия	4	
	Лабораторные занятия	2	
Тема 1.2. Нормативно-правовая база ИБ в Российской Федерации	Обзор ключевых законов. Понятия ПДн, оператора ПДн, КИИ, коммерческой тайны. Ответственность за нарушение законодательства в области ИБ. Работа с текстами законов и проектами регламентов.	**8 из них:**	З3, У3, У6, П3, ОК 03, ОК 09
	Лекционные занятия	2	
	Лабораторные занятия	6	
Раздел 2. Технические основы защиты информации			
Тема 2.1. Криптографические методы защиты информации	Основные понятия криптографии: шифрование, симметричные и асимметричные алгоритмы, электронная подпись (ЭП/ЭЦП), хеш-функции. Применение криптографии для обеспечения конфиденциальности и целостности данных. Практика: использование средств шифрования (VeraCrypt), создание и проверка ЭП, расчет хеш-сумм.	**10 из них:**	З5, У4, П2, ОК 02
	Лекционные занятия	4	
	Лабораторные занятия	6	
Тема 2.2. Защита на уровне операционной системы и сети	Управление доступом: модели DAC, MAC, RBAC. Аутентификация и авторизация. Базовые меры защиты ОС: настройка парольной политики, учетных записей, журналов событий (аудит). Основы сетевой безопасности: понятие МЭ (брандмауэра), анализ сетевых атак (сканирование портов).	**8 из них:**	З4, З6, У2, П1, ОК 02
	Лекционные занятия	2	
	Лабораторные занятия	6	
Раздел 3. Безопасность данных и прикладных систем			
Тема 3.1. Безопасность баз данных и проведение аудита	Угрозы безопасности СУБД: несанкционированный доступ, SQL-инъекции, утечка данных. Базовые механизмы защиты в СУБД: роли, привилегии, шифрование данных, аудитовые журналы.	**10 из них:**	З4, З7, У5, П1, П3, П4, ОК 01, ОК 02, ОК 09, ПК 2.3

	Методика проведения аудита безопасности БД. Работа с чек-листами и регламентами (на основе PCI DSS, ГОСТ).		
	Лекционные занятия	2	
	Лабораторные занятия	8	
Тема 3.2. Основы безопасности в разработке и при работе с ИИ	Безопасность жизненного цикла разработки (Secure SDLC). Уязвимости, специфичные для систем с ИИ: отравление данных, атаки на модели (adversarial attacks), защита интеллектуальной собственности. Разработка инструкции по безопасной работе с конфиденциальными данными в проекте.	**6** **из них:**	З2, З3, У1, У6, П2, П3, ОК 03
	Лекционные занятия	2	
	Лабораторные занятия	4	
Всего:			
Лекции		**16**	
Лабораторные занятия		**32**	
Самостоятельная работа обучающегося		**4**	
Промежуточная аттестация – экзамен		**12**	
Всего		**64**	

3. Условия реализации дисциплины

3.1 Требования к материально-техническому обеспечению

Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

1. Специальное помещение: учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля, промежуточной и государственной итоговой аттестации, оснащенное:

- стандартная учебная мебель (30 посадочных мест);
- стол и стул для преподавателя (по 1 шт.);
- кафедра для лектора (1 шт.);
- доска настенная трехэлементная (1 шт.);
- интерактивная доска (напольная) SMART BOARD (1 шт.);
- мультимедийный проектор NEC (1 шт.);
- ноутбук Asus(1 шт.);
- колонки Genius(1 пара);
- компьютерный студенческий стол (15 шт.);
- компьютерный стол
преподавателя (1 шт.);
- монитор Acer (15 шт.);
- системный блок Kraftway (15 шт.);
- принтер Canon (1 шт.);
- наушники с микрофоном (15 шт.)

2. Помещение для организации самостоятельной и воспитательной работы, оснащенное компьютерной техникой с возможностью подключения к информационно-

телекоммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду организации, оснащенное:

- персональные компьютеры с выходом в Интернет (15 шт.);
- компьютерный студенческий стол (15 шт.);
- стол и стул для преподавателя (по 1 шт.);
- доска настенная трехэлементная (1 шт.);
- интерактивная доска IQBoard;
- мультимедиа проектор Optoma PX 329 DLP;
- акустическая система 2.0 (3 шт.);
- наушники с микрофоном (15 шт.)

3.2. Информационное обеспечение реализации программы

3.2.1. Обязательные печатные и электронные издания

1. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 252 с. — (Профессиональное образование). — ISBN 978-5-534-20154-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567521

2. Организационное и правовое обеспечение информационной безопасности : учебник для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 357 с. — (Профессиональное образование). — ISBN 978-5-534-19107-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561717

3. Козырь, Н. С. Анализ и оценка рисков информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь, В. Н. Хализев. — Москва : Издательство Юрайт, 2025. — 157 с. — (Профессиональное образование). — ISBN 978-5-534-20645-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581503

3.2.2. Дополнительные источники

1. Козырь, Н. С. Аудит информационной безопасности : учебник для среднего профессионального образования / Н. С. Козырь. — Москва : Издательство Юрайт, 2025. — 36 с. — (Профессиональное образование). — ISBN 978-5-534-20505-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/581504

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебник для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — 2-е изд. — Москва : Издательство Юрайт, 2025. — 352 с. — (Профессиональное образование). — ISBN 978-5-534-19384-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580668

3. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542340

3.2.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. www.servernews.ru – информационные материалы о средствах ИТ и средствах обеспечения ИБ
2. www.fstec.ru – сайт ФСТЭК РФ

3. www.infosec.ru – группа компаний Информзащита

4. www.anti-malware.ru – аналитический центр Anti-Malware**3.3 Программное обеспечение**

KasperskyEndpointSecurity для бизнеса Стандартный АО «Лаборатория Касперского», лицензия 1FB6-161215-133553-1-6231.

Microsoft Open License, лицензия 49463448 в составе:

1. Microsoft Windows Professional 7 Russian;
2. Microsoft Office 2010 Russian.

Обучающимся обеспечен доступ к ЭБС «Юрайт», ЭБС «IPRbooks», доступ в электронную информационно-образовательную среду университета, а также доступ к современным профессиональным базам данных и информационным справочным системам.

4. Контроль и оценка результатов освоения дисциплины

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения лабораторных занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Курсовые работы по данной дисциплине учебным планом не предусмотрены.

Результаты обучения	Формы и методы контроля и оценки результатов обучения
Предметные результаты обучения Обучающийся должен **знать/иметь представление:** – З1 – основные понятия, цели и принципы информационной безопасности (конфиденциальность, целостность, доступность, аутентичность, неотказуемость); – З2 – классификацию угроз и уязвимостей информационных систем, источники и виды угроз (внутренние/внешние, преднамеренные/непреднамеренные), типы атак (социальная инженерия, вредоносное ПО, DDoS); – З3 – основы российского законодательства в области ИБ; – З4 – модели и политики управления доступом (DAC, MAC, RBAC), принципы аутентификации, авторизации и аудита (AAA); – З5 – базовые методы и средства криптографической защиты информации (шифрование, ЭЦП, хеширование), их применение для обеспечения конфиденциальности и целостности; – З6 – принципы обеспечения безопасности на различных уровнях: физический, аппаратный, уровень ОС, сетевой, прикладной; – З7 – методику проведения базового аудита безопасности, структуру и содержание типовых регламентов по защите информации, стандартов. **уметь/владеть:** – У1 – идентифицировать основные активы (данные, системы, сервисы) и анализировать связанные с ними риски информационной безопасности в контексте профессиональной деятельности; – У2 – применять базовые меры защиты на уровне рабочей станции и пользователя: настройка	Текущий контроль: - устный опрос; - оценка письменных работ; - защита лабораторных работ; - тестирование (письменное или компьютерное) по разделам; - проверка конспектов; - проектные задания; - решение кейсов; Промежуточная аттестация: - экзамен

парольной политики, работа с антивирусным ПО, настройка брандмауэра, безопасное использование съемных носителей; – У3 – работать с нормативной документацией (политики ИБ, регламенты, инструкции) на русском языке, понимать ключевые положения стандартов ИБ на английском языке; – У4 – использовать основные криптографические средства (средства шифрования дисков, создания ЭЦП, проверки хеш-сумм) для защиты данных; – У5 – проводить элементарную проверку (аудит) настроек безопасности СУБД на предмет соответствия базовым требованиям (сложность паролей, права доступа, журналирование); – У6 – разрабатывать и оформлять простейшие организационно-распорядительные документы в области ИБ (инструкция пользователя, регламент обращения с конфиденциальной информацией). – П1 – оценки защищенности информационной системы или её компонента по заданным критериям; – П2 – применения полученных знаний для обеспечения безопасной работы с персональными и конфиденциальными данными в учебных и модельных профессиональных ситуациях; – П3 – использования нормативно-правовой базы и профессиональной документации для обоснования принимаемых решений в области ИБ; – П4 – проведения элементарных аудиторских проверок настроек систем (в частности, СУБД) с использованием чек-листов и регламентов.	